afm unternehmensgruppe assekuranz-finanz-makler

Datenschutz

afm Notfallpläne

Stand 02-2019

Liebe Kolleginnen und Kollegen,

bitte beachten Sie, dass Sie zunächst selbst eine Fehlerbeurteilung vornehmen sollten und erst nach Erfolglosigkeit Ihre Kollegen oder IT-Service-Mitarbeiter nach folgendem Schema ansprechen.

Jede Störung im Arbeitsablauf bedeutet auch die anschließende Zeit bis zur Wiederaufnahme der Tätigkeit, bis zum abgebrochenen Vorgang oder multipliziert sich mit der Anzahl der involvierten Kollegen, die Sie nach Unterstützung fragen. Bitte haben Sie Respekt vor der Arbeitszeit Ihrer Kollegen.

Falls Sie ansonsten ungehindert weiterarbeiten können, sammeln Sie Ihre IT-Probleme, sprechen diese mit Kollegen ab und übergeben der IT-Administration einmalig alle bekannten Störungen oder Verbesserungswünsche.

Die Geschäftsleitung

Ansprechpartner IT-Administration

Heiko Hallmann
Kaiser-Wilhelm-Str. 9
20355 Hamburg
Tel. 040 532886-132
hallmann@afm-gruppe.de

Stephan Tomfohrde
Kaiser-Wilhelm-Str. 9
20355 Hamburg
Tel. 040 532886-136
tomfohrde@afm-gruppe.de

Mail-Postfach der IT-Abteilung: **hotline@afm-gruppe.de**

Inhalt

1. Allgemeines Vorgehen bei IT-Störungen
2. IT-Ausfall
3. Server-Ausfall
4. Virenbefall
5. IT-Verlust
6. Verstoß gegen Datenschutz
7. Behördenanfragen telefonisch
8. Behördenanfragen vor Ort
9. Reputationsschaden
10. Abmahnungen
11. Datenverlust | versehentliche Löschung

1. Allgemeines Vorgehen bei IT-Störungen

- Stromzufuhr prüfen (Rechner & Monitor, Sichtprüfung der Kontrolllampen)
- Eingabegeräte prüfen (Kabel eingesteckt, sichtbarer Defekt, gegebenenfalls Batterien aus einem anderen, zurzeit ungenutzten Gerät testen, kabelgebundenes Eingabegerät von einem ungenutzten PC anschließen und testen)
- Netzwerkverbindung prüfen (Kabel eingesteckt, im AD: WLAN-Verbindung überprüfen)
- Neustart des Systems (mit Sichtprüfung ungewöhnlicher Anzeigen/Fehlermeldungen, gegebenenfalls Ein-/Ausschalter vorher 5 Sekunden lang gedrückt halten für Zwangsabschaltung des PCs)
- Standardsoftware auf Funktion prüfen (Internetbrowser, dort etwas in einer Suchmaschine googeln, klappt das?)
- Spezialanwendung prüfen (Anmeldung, Funktion)
- Peripherie prüfen (z.B. Anzeigen/Lampen/LEDs am Drucker)
- Bitte ansonsten keine Try & Error Selbstreparaturversuche („Verschlimmbesserung“), dazu ist die IT-Abteilung da

↳ **Kann Störung nicht behoben werden, IT-Administrator verständigen**

Idealerweise protokollieren Sie Ihre Schritte.
Bei ungewöhnlichen Vorfällen (bspw. mehrmaliges „Piepen“ des Rechners beim Start, ungewöhnliche „Flecken/Flimmern“ auf dem Bildschirm) bitte IT-Administration verständigen. Halten Sie eine möglichst genaue Fehlerbeschreibung bereit – die IT kann meist helfen, wenn der Fehler reproduziert werden kann.

2. IT-Ausfall

Die IT arbeitet nicht wie gewohnt, Vorgänge dauern ungewöhnlich lang, Funktionen stehen nicht zur Verfügung, Programme starten nicht, Vorgänge werden nicht abgeschlossen, es besteht keine Netzwerkverbindung, IT fährt nicht hoch, ein Eingabegerät funktioniert nicht mehr, …

- Wie stellt sich der Fehler dar? (z.B. keine Reaktion auf Benutzereingaben/Mausbewegung, keine Antwort vom Server, Netzwerklaufwerke nicht erreichbar)
- Was waren die letzten korrekt funktionierenden Schritte?
- Gibt es für den erkannten Fehler eine Standardreparaturprozedur?
- Bei unerwarteten, unbekannten Fehlern bitte keine Selbstreparaturversuche!
- Ist ein kompetenter Mitarbeiter im Umfeld?
- Ist der Fall bereits von anderen entdeckt und in Bearbeitung?
- Haben andere Mitarbeiter das gleiche Problem?
- Wer ist Ansprechpartner für das aufgetretene IT-Problem?
- Ist der Ansprechpartner gerade erreichbar?
- Kann ich in der Zwischenzeit eine andere produktive Aufgabe erledigen? (Posteingang sortieren, Aktenablage, Mandanten-Telefonate, Besprechung, Besorgungen, …)

↳ **Kann Störung nicht behoben werden, IT-Administrator verständigen**

3. Server-Ausfall

Server sind die zentralen Rechner, die allen Nutzern IT-Dienste innerhalb des Betriebsnetzwerkes zur Verfügung stellen. Zur Verwirrung kann es kommen, da der Begriff Server sowohl als Bezeichnung für die physische Hardware als auch für einen zur Verfügung gestellten Dienst verwendet wird. Z.B. kann ein physischer Server die Dienste Anwendungs-Server, Terminal-Server, Datenbank-Server, Datei-Server, E-Mail-Server und Web-Server beinhalten.

Typische Serverdienste sind beispielsweise: Rechtesystem/Anmeldung, E-Mail, Druck, Datei, …

Meist bemerkt man den Verlust eines Serverdienstes dadurch, dass andere Kollegen zeitgleich ein ähnliches IT-Problem haben. Um mit einem Server arbeiten zu können, braucht man eine logische Verbindung (also angemeldet/authentifiziert) per physischer Verbindung (Netzwerkkabel, WLAN).

Folgende Komponenten sind vom Arbeitsplatz bis zum Serverdienst funktionsfähig notwendig:

- Gestarteter, angemeldeter Rechner
- eingestecktes Netzwerkkabel (in PC und Bodentank oder Wandanschluss)
- Gegenstelle des Kabels „gepatcht“ (d.h. im Verteiler angeschlossen)
- funktionierender Netzwerkverteiler (sog. „Switch“)
- Verkabelung vom Switch zum physischen Server
- dort: funktionierende Netzwerkkarte in laufendem Server mit notwendigen Kapazitäten (d.h. nicht überlastet mit anderen Aufgaben bspw. Backup o.ä.)
- ausgeführter Server-Dienst (bspw. zentrales E-Mail-Programm)

  Sollten die Benutzerrechte in Ordnung sein, ist diese Funktionskette immer Voraussetzung zum ordnungsgemäßen Funktionieren der IT. Eine gestörte Komponente und „… der Server geht nicht …“

Für die Erreichbarkeit von Internet-Diensten muss zudem gewährleistet sein:

- angeschlossene und funktionierende Firewall (zur Sicherheitsüberprüfung des Internetverkehrs)
- angeschlossener und funktionierender Router (als Übergabepunkt ins Internet)
- funktionierende Gegenstelle (sowohl bei Provider als auch entfernter Internet-Server)

Kann Störung nicht behoben werden, IT-Administrator verständigen

Im Regelfall haben Sie als Anwender keine Möglichkeit, Serverdienste zu warten oder wiederherzustellen. Bitte versuchen Sie also, durch möglichst genaue Beschreibung des Fehlers Ihre IT zu informieren.

4. Virenbefall

Viren bzw. Trojaner sind Schadprogramme, die möglichst unbemerkt einen physischen Schaden, eine Ressourcennutzung oder einen Datendiebstahl durchführen. Viren müssen von extern ins System eingeschleust und ausgeführt werden.

Die häufigsten Ursachen sind:

- Ausführen eines unbekannten Programmes als Anhang einer E-Mail oder als Download-Link in einer E-Mail
- Surfen im Internet auf fragwürdigen oder gehackten/gekaperten Web-Seiten ohne ausreichenden Schutz, dabei werden oft Lücken durch fehlende Sicherheits- oder Programm-Updates auf dem PC ausgenutzt
- USB-Sticks, CD-ROM

Bei festgestelltem Virus ist idealerweise unmittelbar das System nicht mehr zu bedienen und zu isolieren (bestenfalls Netzwerkkabel entfernen, sonst Stromkabel ziehen oder PC abschalten) und IT-Administration zu verständigen

Viren verbreiten sich oftmals von alleine, hier hilft jede gewonnene Zeit. Bitte nicht nur einen bestätigten Virenbefall, sondern auch die Verdachtsmomente melden!

- Was waren die letzten Tätigkeiten vor Entdecken der Schadsoftware?
- Welches Verhalten weist auf einen Virus / Schadsoftware hin?
- Wird der Virus von der Antivirensoftware angezeigt?
- Kann eine Autoreparatur durch den Virenscanner erfolgen?
- Welche Software ist betroffen (oder allg. Betriebssystem-Funktion)?
- Netzwerkverbindung trennen
- Bitte keinen Neustart durchführen, System isolieren (Netzwerkstecker ziehen) und in Ruhe lassen
- Wer ist Ansprechpartner in der IT?
- Ist gerade jemand von der IT erreichbar?
- Wenn nein, „hart“ ausschalten (notfalls Stromkabel ziehen oder den Einschalter 5 Sekunden lang gedrückt halten) und nicht mehr hochfahren

5. IT-Verlust

Kann bei normalem, sorgfältigem Umgang jedem passieren. Schlimm ist, wenn nicht sofort reagiert wird und entsprechende Lösch-/Vorsichtsmaßnahmen durchgeführt werden. Insbesondere bei Messen-, Kundenbesuchen, im Kfz, ÖPNV oder bei Hotelübernachtungen.

- Welches Gerät?
- Wann wurde der Verlust bemerkt?
- Wo war der letzte bekannte Ort vor dem Verlust?
- Ist das Gerät bei möglicher Bedienung durch Dritte passwortgeschützt und der Datenträger zusätzlich verschlüsselt?
- Waren vertrauliche/personenbezogene Daten auf dem Gerät? Welche? Bestehen aktive Verbindungen, z.B. per E-Mail-Client oder zum TerminalServer? Sind Zugangsdaten im Web-Browser, Mail-Client oder für WLAN-Verbindungen gespeichert worden?

IT-Administrator und Datenschutzbeauftragten verständigen

Anschließend nach Absprache Fernlöschung veranlassen sowie ggf. den Vorfall bei der Polizei und der Versicherung melden.

6. Verstoß gegen Datenschutz

Sollte Ihnen ein Verstoß gegen das Datenschutzgesetz auffallen oder selbst passieren, muss umgehend gehandelt werden. Hier ist proaktives Handeln erforderlich, am schlimmsten ist, wenn der Fehler vertuscht oder von extern zuerst erkannt wird.

- Welcher Mandant ist betroffen?
- Welche Daten sind betroffen?
- Wer hat den Datenverstoß verursacht (auch Fehlfunktion von Software, Kommunikation)
- Technische Ursache des Datenverstoßes?
- Besteht ein möglicher Schaden für die betroffene Person?

Geschäftsführung und Datenschutzbeauftragten informieren
Weiter mit Checkliste Meldung Datenpanne!

7. Behördenanfragen telefonisch

Grundsätzlich gilt: keine vertraulichen Daten per Telefon an nicht eindeutig authentifizierte Personen. Lassen Sie sich das Begehren IMMER schriftlich unter Angabe der Behörde, der gesetzlichen Grundlage, des Aktenzeichens und Ansprechpartners mitteilen.

Keine Behörde wird Sie auffordern, telefonisch sensible Daten zu übermitteln. Achten Sie hierzu auch auf unrechtmäßige Versuche von „Social Hackern“, im Namen einer Behörde Druck auszuüben.

- Name, Behörde, Vorgesetzter, Amtszeichen/-notiz notieren
- Um welchen Fall handelt es sich, auf welcher gesetzlichen Grundlage wird dieser ausgeführt?
- Wer ist betroffene Person?
- Keinen Schriftsatz oder E-Mail eigenmächtig ohne vorherige Freigabe eines Vorgesetzten verfassen oder versenden!

Geschäftsführung und Datenschutzbeauftragten informieren

8. Behördenanfragen vor Ort

Steuerfahndung, Zoll oder Strafverfolgungsbehörden können sich Zutritt zu den Büroräumen verschaffen. Dazu benötigen diese eine gerichtliche Anordnung. Bitte lassen Sie sich den entsprechenden Durchsuchungstitel zeigen und geben Sie ohne weiteren Beistand oder Zeugen keinerlei Auskunft. Verlangen Sie einen Anwalt.

- Name, Behörde des Verantwortlichen nennen lassen
- Richterlicher Durchsuchungsbefehl vorhanden? Wenn nein, Kooperation zeigen, aber Zugang verweigern unter Hinweis auf Datenschutzbestimmungen im Büro
- Rechtsgrundlage prüfen und Titel zeigen lassen
- Keine mündlichen Auskünfte ohne Rechtsbeistand geben (außer Nennung von Namen, Funktion, Anschrift, Zeigen von Personalausweis)
- nicht auf Beteuerungen und Versprechungen eingehen

umgehend Geschäftsführung und Datenschutzbeauftragten informieren

9. Telekommunikation und Internet

Auch bekannt unter dem Namen „Cybermobbing“. Darunter fallen alle Aussagen, die den Ruf des Unternehmens oder darin handelnder Personen schaden können.

Reputationsschäden sind kein Kavaliersdelikt und sollten im Regelfall auch zur Anzeige gebracht werden. Insbesondere die anonyme und flüchtige Informationsverbreitung über soziale Medien (vgl. „Shit-Storm“) kann durch virale Effekte unüberschaubare Dimensionen annehmen, die bis zur Schädigung des Geschäftsbetriebes durch Vertrauensverlust reichen kann.

- In welchem Medium wurde der Schaden festgestellt (Twitter, Facebook, Website, …)
- Sind Personen des Unternehmens genannt?
- Inhalt des Schadens festhalten (bspw. durch Kopieren des Textes, Speichern des Bildes)
- Kann der Autor festgestellt werden (auch Pseudonym)?
- Screenshots anfertigen (das Speichern der URL alleine reicht nicht!)
- Standard-Text unter dem Firmen-Account im jeweiligen Medium posten
- Weiter im Medium über den Fall in regelmäßigen Abständen kommunizieren (spätestens alle 24 Stunden)
- Je nach Zeitleiste kann die gleiche Meldung auch in Abständen wiederholt gepostet werden
- Außer Offenheit und Transparenz wird keine andere Strategie zum Erfolg führen. Jede weitere PR-Standardantwort wird den Fall eher verschlimmern.
- Lösch-/Sperranfrage an das Medium stellen
- Anwalt kontaktieren, Unterlassungsklage vorbereiten
- Polizeiliche Anzeige erstatten

Geschäftsführung und Datenschutzbeauftragten informieren
Anschließend nach Absprache ggf. Anwalt kontaktieren, Unterlassungsklage vorbereiten, polizeiliche Anzeige erstatten

10. Abmahnungen

Ein kleiner falscher Eintrag im Impressum, eine fehlgeleitete E-Mail, eine Auskunft an eine falsche Person, ein nicht lizensiertes oder gekennzeichnetes Bild auf der Website oder im Prospekt, eine urheberrechtlich geschützte Textpassage oder nicht freigegebenes Verwenden eines Logos/Markenrechtes können unmittelbar zu einer Abmahnung führen. Grundsätzlich ist das kein Weltuntergang – was in keinem Fall passieren darf, ist es, die im Schreiben enthaltene Frist verstreichen zu lassen.

- Vorwurf klären und prüfen
- Aktenzeichen und gegnerische Kanzlei/Anwalt notieren

Geschäftsführung informieren

- Anwaltliches Schreiben anfertigen lassen (Achtung Fristen)
- Anwaltliches Schreiben so absenden, dass die Gegenseite den Inhalt vor Ablauf der Frist erhält
- Bitte keinerlei selbstständige oder nicht abgestimmte Kommunikation mit der Gegenpartei
- Keine nicht abgestimmten Tatsachen schaffen
  bspw. kann das Entfernen einer Ursache als Schuldeingeständnis indiziert werden
- Vor Ablauf der Frist den Vorwurf entkräften oder die Ursache entfernen

11. Datenverlust | versehentliche Löschung

Unabsichtliche Datenlöschung ist wohl die häufigste Ursache des Datenverlustes. Unkonzentriertheit, unsaubere Abläufe, Bequemlichkeit oder Fehlbedienung können zu Datenverlusten führen. Grundsätzlich gilt auch hier:

- überlegt und professionell gehandelt erhöht die Wahrscheinlichkeit der Datenrettung
- jeder „Try & Error“ führt zur Verschlimmbesserung

Fehler passieren jedem. Bitte vertuschen Sie also nichts sondern helfen der IT zur professionellen Datenrettung.

- Bei Entdecken der Datenlöschung: Sofort Finger weg von Maus und Tastatur! Nicht die Zeit, sondern die nächste Aktion bestimmt den weiteren Verlauf der Datenrettung
- Nur weiter Vorgehen, wenn der nächste Schritt bewusst in jedem Fall zur Datenrettung führt
- Notieren: Was waren die letzten Schritte?
- Welche Daten sind vermutlich gelöscht worden?
- Mit welcher Software?
- Sind die Daten noch an einem anderen Ort (bspw. Ausdruck, Akten, Vertrag) vollständig erfasst?
- Ist das Dokument/Formular noch an einem anderen Ort geöffnet?

IT-Administrator verständigen

Bitte im Ausnahmefall nur Kollegen, die offiziell den notwendigen Sachverstand haben, verständigen.

- Planung der Wiederherstellung in Abwägung des Aufwandes
  bspw. kann es sinnvoller sein, den einzelnen Datensatz wieder neu von Hand zu erfassen, als ein Backup einzuspielen